

THE t -METRIC MAHLER MEASURES OF SURDS OF RATIONAL NUMBERS

JONAS JANKAUSKAS AND CHARLES L. SAMUELS

ABSTRACT. A. Dubickas and C. Smyth introduced the metric Mahler measure

$$M_1(\alpha) = \inf \left\{ \sum_{n=1}^N M(\alpha_n) : N \in \mathbb{N}, \alpha_1 \cdots \alpha_N = \alpha \right\},$$

where $M(\alpha)$ denotes the usual (logarithmic) Mahler measure of $\alpha \in \overline{\mathbb{Q}}$. This definition extends in a natural way to the t -metric Mahler measure by replacing the sum with the usual L_t norm of the vector $(M(\alpha_1), \dots, M(\alpha_N))$ for any $t \geq 1$. For $\alpha \in \mathbb{Q}$, we prove that the infimum in $M_t(\alpha)$ may be attained using only rational points, establishing an earlier conjecture of the second author. We show that the natural analogue of this result fails for general $\alpha \in \overline{\mathbb{Q}}$ by giving an infinite family of quadratic counterexamples. As part of this construction, we provide an explicit formula to compute $M_t(D^{1/k})$ for a squarefree $D \in \mathbb{N}$.

1. INTRODUCTION

Let f be a polynomial with complex coefficients given by

$$f(z) = a \cdot \prod_{n=1}^N (z - \alpha_n).$$

Recall that the (*logarithmic*) Mahler measure M of f is defined by

$$M(f) = \log |a| + \sum_{n=1}^N \log^+ |\alpha_n|.$$

If α is a non-zero algebraic number, the (*logarithmic*) Mahler measure $M(\alpha)$ of α is defined as the Mahler measure of the minimal polynomial of α over \mathbb{Z} .

It is a consequence of a theorem of Kronecker that $M(\alpha) = 0$ if and only if α is a root of unity. In a famous 1933 paper, D.H. Lehmer [5] asked whether there exists a constant $c > 0$ such that $M(\alpha) \geq c$ in all other cases. He could find no algebraic number with Mahler measure smaller than that of

$$\ell(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1,$$

which is approximately $0.16\dots$. Although the best known general lower bound is

$$M(\alpha) \gg \left(\frac{\log \log \deg \alpha}{\log \deg \alpha} \right)^3,$$

2010 *Mathematics Subject Classification*. 11R04, 11R09 (Primary), 11C08, 12E05 (Secondary).
Key words and phrases. Weil height, Mahler measure, metric Mahler measure, Lehmer's problem.
 The first author was supported by the Lithuanian Research Council (student research support project) during his visit to the IRMACS Centre, Simon Fraser University.
 The second author was supported by NSERC of Canada.

due to Dobrowolski [2], uniform lower bounds have been established in many special cases (see [1, 14, 15], for instance). Furthermore, numerical evidence provided, for example, in [6–9] suggests there exists such a constant c .

Conjecture 1.1 (Lehmer’s conjecture). *There exists a real number $c > 0$ such that if $\alpha \in \overline{\mathbb{Q}}^\times$ is not a root of unity then $M(\alpha) \geq c$.*

For an algebraic number α , Dubickas and Smyth [3] introduced the *metric Mahler measure* $M_1(\alpha)$ by

$$(1.1) \quad M_1(\alpha) = \inf \left\{ \sum_{n=1}^N M(\alpha_n) : N \in \mathbb{N}, \alpha_n \in \overline{\mathbb{Q}}^\times, \alpha = \prod_{n=1}^N \alpha_n \right\}.$$

Here, the infimum is taken over all ways to write α as a product of algebraic numbers. The advantage of M_1 over M is that it satisfies the triangle inequality

$$M_1(\alpha\beta) \leq M_1(\alpha) + M_1(\beta)$$

for all algebraic numbers α and β . In view of this observation, M_1 is well-defined on the quotient group $G = \overline{\mathbb{Q}}^\times / \text{Tor}(\overline{\mathbb{Q}}^\times)$, and the map $(\alpha, \beta) \mapsto M_1(\alpha\beta^{-1})$ defines a metric on G . This metric induces the discrete topology if and only if Lehmer’s conjecture is true.

The metric Mahler measure M_1 is only a special case of the t -metric Mahler measures, which are defined for $t \geq 1$ by

$$M_t(\alpha) = \inf \left\{ \left(\sum_{n=1}^N M(\alpha_n)^t \right)^{1/t} : N \in \mathbb{N}, \alpha_n \in \overline{\mathbb{Q}}^\times, \alpha = \prod_{n=1}^N \alpha_n \right\}.$$

In addition, the ∞ -metric Mahler measure of α is defined by

$$M_\infty(\alpha) = \inf \left\{ \max_{1 \leq n \leq N} \{M(\alpha_n)\} : N \in \mathbb{N}, \alpha_n \in \overline{\mathbb{Q}}^\times, \alpha = \prod_{n=1}^N \alpha_n \right\}.$$

The t -metric Mahler measures were introduced and studied in [12, 13]. It follows from the results of [12] that these functions have analogues of the triangle inequality

$$M_t(\alpha\beta)^t \leq M_t(\alpha)^t + M_t(\beta)^t \quad \text{and} \quad M_\infty(\alpha\beta) \leq \max\{M_\infty(\alpha), M_\infty(\beta)\}$$

Hence, the map $(\alpha, \beta) \mapsto M_t(\alpha\beta^{-1})$ defines a metric on G that induces the discrete topology if and only if Lehmer’s conjecture is true.

If $t \in [1, \infty]$ and $\alpha \in \overline{\mathbb{Q}}$, we say that *the infimum in $M_t(\alpha)$ is attained by $\alpha_1, \dots, \alpha_N$* if we have that

$$\alpha = \alpha_1 \cdots \alpha_N \quad \text{and} \quad M_t(\alpha) = \begin{cases} \left(\sum_{n=1}^N M(\alpha_n)^t \right)^{1/t} & \text{if } t < \infty \\ \max_{1 \leq n \leq N} \{M(\alpha_n)\} & \text{if } t = \infty. \end{cases}$$

If S is any subset of $\overline{\mathbb{Q}}$, we say *the infimum in $M_t(\alpha)$ is attained in S* if there exist points $\alpha_1, \dots, \alpha_N \in S$ that attain the infimum in $M_t(\alpha)$.

It is not immediately obvious that $M_t(\alpha)$ is attained for all values of α and t . Dubickas and Smyth [3] conjectured that the infimum in $M_1(\alpha)$ is always attained a fact later proved by the second author [11]. More specifically, if K_α is the Galois closure of $\mathbb{Q}(\alpha)$ over \mathbb{Q} and

$$\text{Rad}(K_\alpha) = \{\gamma \in \overline{\mathbb{Q}} : \gamma^n \in K_\alpha \text{ for some } n \in \mathbb{N}\},$$

then the infimum in $M_1(\alpha)$ is attained in $\text{Rad}(K_\alpha)$. Using the same method, this result was generalized for all t -metric Mahler measures in [12]. That is, for every $t \geq 1$, the infimum in $M_t(\alpha)$ is attained in $\text{Rad}(K_\alpha)$.

It is natural to ask if these results can be improved, having a smaller set S in place of $\text{Rad}(K_\alpha)$. In particular, for each $\alpha \in \overline{\mathbb{Q}}$, we would like to identify a set S_α whose points generate a finite extension of \mathbb{Q} and the infimum in $M_t(\alpha)$ is attained in S_α for all t . This problem is of considerable importance if we hope to compute exact values of $M_t(\alpha)$. For example, Conjecture 2.1 of [13] predicts that, if α is rational, then the infimum in $M_t(\alpha)$ is attained in \mathbb{Q} . With this assumption, it is possible to graph some examples of the function $t \mapsto M_t(\alpha)$ where $\alpha \in \mathbb{Q}$.

It follows from [3] and [4] that Conjecture 2.1 of [12] holds for $t = 1$ and $t = \infty$. Unfortunately, these methods seem genuinely distinct and cannot be easily generalized to handle all values of t and α . As our first result, we prove this conjecture for all $t \geq 1$.

Theorem 1.2. *If α is a non-zero rational number and $t \in [1, \infty]$ then the infimum in $M_t(\alpha)$ is attained in \mathbb{Q} .*

Our next question is whether Theorem 1.2 can be extended to arbitrary algebraic numbers α . In view of Theorem 1.2, one might suspect that the infimum in $M_t(\alpha)$ is always attained in K_α . This turns out to be false, however, as we are able to produce an infinite family of quadratic counterexamples. More specifically, if D is a square-free positive integer, we show precisely when $M_t(\sqrt{D})$ is attained in $K_{\sqrt{D}} = \mathbb{Q}(\sqrt{D})$.

Theorem 1.3. *Suppose that p_1, \dots, p_L are distinct primes written in decreasing order, $D = p_1 \cdots p_L$, and $t \in (1, \infty]$. The infimum in $M_t(\sqrt{D})$ is attained in $\mathbb{Q}(\sqrt{D})$ if and only if $D < p_1^2$. In this situation, the infimum is attained by points*

$$\sqrt{\frac{p_1}{p_2 \cdots p_L}}, p_2, \dots, p_L \in \mathbb{Q}(\sqrt{D}),$$

and we have that

$$M_t(\sqrt{D}) = \begin{cases} \left(\sum_{\ell=1}^L (\log p_\ell)^t \right)^{1/t} & \text{if } t \in (1, \infty) \\ \log p_1 & \text{if } t = \infty. \end{cases}$$

Theorem 1.3 enables the construction of infinitely many integers D such that $M_t(\sqrt{D})$ is not attained in $K_{\sqrt{D}} = \mathbb{Q}(\sqrt{D})$ for any $t > 1$. Theorem 1.4 below gives a set of points that attain the infimum in $M_t(\alpha)$ for algebraic numbers $\alpha = D^{1/k}$, where $D > 0$ is a square-free integer.

Theorem 1.4. *If p_1, \dots, p_L are distinct primes, $D = p_1 \cdots p_L$, and $t \in [1, \infty]$, then the infimum in $M_t(D^{1/k})$ is attained by $p_1^{1/k}, \dots, p_L^{1/k}$ and*

$$M_t(D^{1/k}) = \begin{cases} \left(\sum_{\ell=1}^L (\log p_\ell)^t \right)^{1/t} & \text{if } t \in [1, \infty) \\ \max_{1 \leq \ell \leq L} \{\log p_\ell\} & \text{if } t = \infty. \end{cases}$$

As an example, for $D = 30 = 2 \cdot 3 \cdot 5$, Theorem 1.4 asserts that $M_t(\sqrt{30})$ is attained by $\sqrt{2}, \sqrt{3}, \sqrt{5}$, and

$$M_t(\sqrt{30})^t = (\log 5)^t + (\log 3)^t + (\log 2)^t.$$

While it is obvious that $\sqrt{2}, \sqrt{3}, \sqrt{5} \notin \mathbb{Q}(\sqrt{30})$, the infimum in $M_t(\sqrt{30})$ might be attained by some distinct set of points in $\mathbb{Q}(\sqrt{30})$. Theorem 1.3 excludes any such possibilities.

If we take $D = 42 = 2 \cdot 3 \cdot 7$, Theorem 1.4 establishes that $M_t(\sqrt{42})$ is attained by $\sqrt{2}, \sqrt{3}, \sqrt{7}$, and

$$M_t(\sqrt{42})^t = (\log 7)^t + (\log 3)^t + (\log 2)^t.$$

Nonetheless, Theorem 1.3 identifies the slightly more subtle points $\sqrt{7/6}, 3, 2 \in \mathbb{Q}(\sqrt{42})$ that also attain the infimum in $M_t(\sqrt{42})$. In this example, we note that the infimum is not attained by a unique set.

At first glance, one might think that the infimum in $M_t(\sqrt{D})$ can be attained only by rational numbers and their square roots. This intuition is misleading, however, as we see in the following example. Let $t = \infty$ and take $D = 21 = 7 \cdot 3$. We know from Theorem 1.3 that the infimum in $M_t(\sqrt{21})$ is attained by the points $\sqrt{7/3}, 3 \in \mathbb{Q}(\sqrt{21})$ and

$$M_t(\sqrt{21})^t = (\log 7)^t + (\log 3)^t.$$

Now consider

$$(1.2) \quad \sqrt{21} = (-1) \cdot \left(\frac{7 + \sqrt{21}}{2} \right) \cdot \left(\frac{3 - \sqrt{21}}{2} \right),$$

and we verify easily that

$$M \left(\frac{7 + \sqrt{21}}{2} \right) = \log 7 \quad \text{and} \quad M \left(\frac{3 - \sqrt{21}}{2} \right) < \log 7.$$

In other words, $M_\infty(\sqrt{21})$ is attained by the points on the right hand side of (1.2) and these points belong to $\mathbb{Q}(\sqrt{21})$. It is important to note that $M((3 - \sqrt{21})/2) > \log 3$, so these points cannot be used to attain the infimum in $M_t(\sqrt{21})$ for other values of t . Nonetheless, this example illustrates that the infimum in $M_t(\sqrt{D})$ may be attained by using distinct non-trivial sets of points contained in $\mathbb{Q}(\sqrt{D})$.

We would like to conclude with the following question.

Question 1.5. *Is the infimum in $M_t(\alpha)$ always attained by points $\alpha_1, \dots, \alpha_N$ such that $[\mathbb{Q}(\alpha_n) : \mathbb{Q}] \leq [\mathbb{Q}(\alpha) : \mathbb{Q}]$ for all n ?*

According to Theorem 1.4, the answer is 'yes' when α is a surd, although we know of little other evidence.

2. THE RATIONAL CASE

Recall that the (*logarithmic*) *Weil height* of an algebraic number α is given by

$$h(\alpha) = \frac{M(\alpha)}{\deg \alpha}.$$

It is well-known that if ζ is a root of unity, then $h(\alpha) = h(\zeta\alpha)$ so that h is well-defined on our quotient group G . Furthermore, if n is an integer, then we have that $h(\alpha^n) = |n| \cdot h(\alpha)$. Also recall that a surd is an algebraic number α such that $\alpha^n \in \mathbb{Q}$ for some positive integer n .

Suppose now that F is any number field containing the algebraic number α . Further assume that K is an extension of F which is Galois over \mathbb{Q} . We set

$$G = \text{Gal}(K/\mathbb{Q}) \quad \text{and} \quad H = \text{Gal}(K/F),$$

and let S be a set of left coset representatives of H in G . Recall that the *norm of α from F to \mathbb{Q}* is given by

$$\text{Norm}_{F/\mathbb{Q}}(\alpha) = \prod_{\sigma \in S} \sigma(\alpha).$$

It follows from standard Galois Theory that $\text{Norm}_{F/\mathbb{Q}}$ is a homomorphism from F to \mathbb{Q} which does not depend on the choice of K or S . In addition, if E is any extension of F , then it is easily verified that

$$(2.1) \quad \text{Norm}_{E/\mathbb{Q}}(\alpha) = \text{Norm}_{F/\mathbb{Q}}(\alpha)^{[E:F]}.$$

We begin our proof of Theorem 1.2 with a lemma that relates the Mahler measure of a surd to the Mahler measure of its norm.

Lemma 2.1. *If γ is a surd then $M(\gamma) = M(\text{Norm}_{\mathbb{Q}(\gamma)/\mathbb{Q}}(\gamma))$.*

Proof. Since γ is a surd, its conjugates over \mathbb{Q} are given by

$$\{\zeta_1\gamma, \zeta_2\gamma, \dots, \zeta_M\gamma\}$$

where $M = \deg \gamma$ and ζ_m are roots of unity. It now follows that

$$\gamma^M \prod_{m=1}^M \zeta_m = \text{Norm}_{\mathbb{Q}(\gamma)/\mathbb{Q}}(\gamma) \in \mathbb{Q}.$$

Since $\text{Norm}_{\mathbb{Q}(\gamma)/\mathbb{Q}}(\gamma)$ is clearly a rational number, we have that

$$M(\text{Norm}_{\mathbb{Q}(\gamma)/\mathbb{Q}}(\gamma)) = h\left(\gamma^M \prod_{m=1}^M \zeta_m\right) = M \cdot h(\gamma) = \deg \gamma \cdot h(\gamma) = M(\gamma)$$

completing the proof. \square

In our proof of Theorem 1.2, it will be necessary to replace an arbitrary representation $\alpha = \alpha_1 \cdots \alpha_N$ with another representation of $\alpha = \beta_1 \cdots \beta_N$ that uses only rational numbers and satisfies

$$\sum_{n=1}^N M(\beta_n)^t \leq \sum_{n=1}^N M(\alpha_n)^t.$$

Our next lemma provides us with the necessary elementary number theoretic tools to do this.

Lemma 2.2. *Suppose that m, r_1, \dots, r_N are positive integers such that*

$$m \mid \prod_{n=1}^N r_n.$$

For $1 \leq n \leq N$, recursively define the points m_n by

$$(2.2) \quad m_1 = \gcd(r_1, m) \quad \text{and} \quad m_n = \gcd\left(r_n, \frac{m}{\prod_{i=1}^{n-1} m_i}\right).$$

Then we have that

$$m = \prod_{n=1}^N m_n.$$

Before we provide the proof of Lemma 2.2, we make one clarification regarding the definition of m_n . Naively, it would appear that

$$\frac{m}{\prod_{i=1}^{n-1} m_i}$$

is not necessarily an integer, so that taking its greatest common divisor with another integer might not be well-defined. However, we note immediately that $m_1 \mid m$, which also implies that m_2 is well-defined. Then clearly we have that $m_2 \mid m/m_1$ implying that m_3 is also well-defined. As we can see, it follows inductively that

$$m_n \mid \frac{m}{\prod_{i=1}^{n-1} m_i}$$

for all $1 \leq n \leq N$, meaning, in particular, that m_n is well-defined for all such n . Now we may proceed with the proof of Lemma 2.2.

Proof of Lemma 2.2. We will assume that $m \neq \prod_{n=1}^N m_n$ and find a contradiction. Since the product $\prod_{n=1}^N m_n$ divides m , there must exist a prime number p for which

$$(2.3) \quad \nu_p(m) > \sum_{j=1}^N \nu_p(m_j),$$

where $\nu_p(x)$ denotes the highest power of p dividing the integer x . It now follows that

$$\nu_p(m_n) < \nu_p(m) - \sum_{j=1}^{n-1} \nu_p(m_j) = \nu_p\left(\frac{m}{\prod_{j=1}^{n-1} m_j}\right)$$

for every $n \in \{1, \dots, N\}$. Hence, the definition of m_n implies that

$$\nu_p(m_n) = \min \left\{ \nu_p(r_n), \nu_p\left(\frac{m}{\prod_{j=1}^{n-1} m_j}\right) \right\} = \nu_p(r_n)$$

for every $n \in \{1, \dots, N\}$. It now follows from (2.3) that $\nu_p(m) > \sum_{n=1}^N \nu_p(r_n)$, contradicting our assumption that m divides $\prod_{n=1}^N r_n$. \square

Now that we have established our key lemmas, we may now proceed with the proof of Theorem 1.2.

Proof of Theorem 1.2. As we have noted in the introduction, the case $t = \infty$ is known [4], so we proceed immediately to the situation where $1 \leq t < \infty$.

We may assume without loss of generality that $\alpha > 0$. Since α is rational, there exist positive integers m and m' such that $\gcd(m, m') = 1$ and $\alpha = m/m'$. Furthermore, by the results of [12], there exist surds $\alpha_1, \dots, \alpha_N$ such that

$$(2.4) \quad \alpha = \alpha_1 \cdots \alpha_N \quad \text{and} \quad M_t(\alpha)^t = \sum_{n=1}^N M(\alpha_n)^t.$$

Let K be a number field containing $\alpha_1, \dots, \alpha_N$. Now we may take the norm from K to \mathbb{Q} of both sides of the first equation in (2.4). We apply (2.1) and the fact that the $\text{Norm}_{K/\mathbb{Q}}$ is a homomorphism to establish that

$$\left(\frac{m}{m'}\right)^{[K:\mathbb{Q}]} = \prod_{n=1}^N \text{Norm}_{K/\mathbb{Q}}(\alpha_n) = \prod_{n=1}^N (\text{Norm}_{\mathbb{Q}(\alpha_n)/\mathbb{Q}}(\alpha_n))^{[K:\mathbb{Q}(\alpha_n)]}.$$

Suppose further that, for each $1 \leq n \leq N$, r_n and s_n are relatively prime positive integers such that

$$\frac{r_n}{s_n} = \pm \text{Norm}_{\mathbb{Q}(\alpha_n)/\mathbb{Q}}(\alpha_n).$$

Therefore, we have that

$$\left(\frac{m}{m'}\right)^{[K:\mathbb{Q}]} = \pm \prod_{n=1}^N \left(\frac{r_n}{s_n}\right)^{[K:\mathbb{Q}(\alpha_n)]}.$$

It is obvious that $[K:\mathbb{Q}(\alpha_n)] \mid [K:\mathbb{Q}]$ so we obtain that

$$m^{[K:\mathbb{Q}]} \mid \left(\prod_{n=1}^N r_n\right)^{[K:\mathbb{Q}]} \quad \text{and} \quad m'^{[K:\mathbb{Q}]} \mid \left(\prod_{n=1}^N s_n\right)^{[K:\mathbb{Q}]}.$$

It follows from elementary number theory facts that

$$(2.5) \quad m \mid \prod_{n=1}^N r_n \quad \text{and} \quad m' \mid \prod_{n=1}^N s_n.$$

Setting up the hypotheses of Lemma 2.2, we define recursive sequences corresponding to m and m' . First set

$$m_1 = \gcd(r_1, m) \quad \text{and} \quad m_n = \gcd\left(r_n, \frac{m}{\prod_{i=1}^{n-1} m_i}\right)$$

and

$$m'_1 = \gcd(s_1, m') \quad \text{and} \quad m'_n = \gcd\left(s_n, \frac{m'}{\prod_{i=1}^{n-1} m'_i}\right)$$

so we clearly have that

$$(2.6) \quad |r_n| \geq |m_n| \quad \text{and} \quad |s_n| \geq |m'_n|.$$

Applying Lemma 2.2, we have that

$$m = \prod_{n=1}^N m_n \quad \text{and} \quad m' = \prod_{n=1}^N m'_n$$

so that

$$(2.7) \quad \alpha = \frac{m}{m'} = \prod_{n=1}^N \frac{m_n}{m'_n}.$$

Now it follows from the definition of $M_t(\alpha)$ that

$$(2.8) \quad M_t(\alpha)^t \leq \sum_{n=1}^N M\left(\frac{m_n}{m'_n}\right)^t,$$

so we must show that the right hand side of (2.8) is also a lower bound for $M_t(\alpha)^t$.

To see this, note that by Lemma 2.1, we have that

$$M(\alpha_n) = M(\text{Norm}_{\mathbb{Q}(\alpha_n)/\mathbb{Q}}(\alpha_n)) = M\left(\frac{r_n}{s_n}\right)$$

for all $1 \leq n \leq N$. We have assumed that r_n and s_n are relatively prime, so it follows from known facts about the Mahler measure that

$$M(\alpha_n) = \log \max\{|r_n|, |s_n|\}.$$

Then applying (2.6), we find that

$$M(\alpha_n) \geq \log \max\{|m_n|, |m'_n|\} \geq M\left(\frac{m_n}{m'_n}\right),$$

and consequently,

$$M_t(\alpha)^t = \sum_{n=1}^N M(\alpha_n)^t \geq \sum_{n=1}^N M\left(\frac{m_n}{m'_n}\right)^t.$$

Combining this with (2.7) and (2.8), the result follows. \square

3. THE QUADRATIC CASE

Our first lemma gives one particular set of points that attain the infimum in $M_t(\sqrt{D})$ for all $t \in [1, \infty]$. When $t > 1$, we can also identify the Mahler measures of any points $\alpha_1, \dots, \alpha_N$ attaining the infimum in $M_t(D^{1/k})$.

Lemma 3.1. *Suppose that p_1, \dots, p_L are distinct primes written in decreasing order, $D = p_1 \cdots p_L$, $t \in [1, \infty)$, and $k \in \mathbb{N}$. The infimum in $M_t(D^{1/k})$ is attained by $p_1^{1/k}, \dots, p_L^{1/k}$ and*

$$M_t(D^{1/k})^t = \sum_{\ell=1}^L (\log p_\ell)^t.$$

If $t > 1$ and $\alpha_1, \dots, \alpha_N$ are algebraic numbers attaining the infimum in $M_t(D^{1/k})$ then $N \geq L$. Moreover, it is possible to relabel the elements $\alpha_1, \dots, \alpha_N$ so that

- (i) $M(\alpha_n) = \log p_n$ for all $n \leq L$, and
- (ii) $M(\alpha_n) = 0$ for all $n > L$.

In particular, $M(\alpha_n) \leq \log p_1$ for all n .

Proof. We certainly have that $D^{1/k} = p_1^{1/k} \cdots p_L^{1/k}$, and by the definition of M_t , we know that

$$M_t(D^{1/k})^t \leq \sum_{\ell=1}^L M(p_\ell^{1/k})^t.$$

For each ℓ , we know that $x^k - p_\ell$ vanishes at $p_\ell^{1/k}$ and is irreducible by Eisenstein's criterion, so that $M(p_\ell^{1/k}) = M(x^k - p_\ell) = \log p_\ell$. Hence, we find that

$$(3.1) \quad M_t(D^{1/k})^t \leq \sum_{\ell=1}^L (\log p_\ell)^t.$$

To prove the first statement of the lemma, it is now sufficient to show that

$$(3.2) \quad M_t(D^{1/k})^t \geq \sum_{\ell=1}^L (\log p_\ell)^t.$$

Now suppose $\alpha_1, \dots, \alpha_N \in \overline{\mathbb{Q}}$ attain the infimum in $M_t(D^{1/k})$ and select a number field K containing $D^{1/k}, \alpha_1, \dots, \alpha_N$. By definition, we know that $D^{1/k} = \alpha_1 \cdots \alpha_N$. Using the fact that $\text{Norm}_{K/\mathbb{Q}}$ is a multiplicative homomorphism, we obtain that

$$\text{Norm}_{K/\mathbb{Q}}(D^{1/k}) = \prod_{n=1}^N \text{Norm}_{K/\mathbb{Q}}(\alpha_n)$$

so that

$$(3.3) \quad \left(\text{Norm}_{\mathbb{Q}(D^{1/k})/\mathbb{Q}}(D^{1/k}) \right)^{[K:\mathbb{Q}(D^{1/k})]} = \prod_{n=1}^N \left(\text{Norm}_{\mathbb{Q}(\alpha_n)/\mathbb{Q}}(\alpha_n) \right)^{[K:\mathbb{Q}(\alpha_n)]}.$$

Each of the above norms is a rational number. Hence, for each n , there exist positive relatively prime integers r_n and s_n such that

$$|\text{Norm}_{\mathbb{Q}(\alpha_n)/\mathbb{Q}}(\alpha_n)| = \frac{r_n}{s_n}.$$

Again using Eisenstein's Criterion, we know that $x^k - D$ is the minimal polynomial of $D^{1/k}$ over \mathbb{Q} , implying that $|\text{Norm}_{\mathbb{Q}(D^{1/k})/\mathbb{Q}}(D^{1/k})| = D$. Substituting these values into (3.3), we find that

$$(3.4) \quad D^{[K:\mathbb{Q}(D^{1/k})]} = \prod_{n=1}^N \left(\frac{r_n}{s_n} \right)^{[K:\mathbb{Q}(\alpha_n)]}.$$

For each n , α_n has minimal polynomial of the form

$$\hat{f}_n(x) = x^d + \frac{a_{d-1}}{b_{d-1}}x^{d-1} + \cdots + \frac{a_1}{b_1}x \pm \frac{r_n}{s_n}$$

over \mathbb{Q} for integers $a_1, \dots, a_{d-1}, b_1, \dots, b_{d-1}$ with $b_i \neq 0$ and $(a_i, b_i) = 1$. Hence, its minimal polynomial over \mathbb{Z} is given by

$$f_n(x) = \text{lcm}(s_n, b_{d-1}, \dots, b_1) \cdot x^d + \cdots \pm r_n \cdot \text{lcm}(s_n, b_{d-1}, \dots, b_1)$$

and its Mahler measure satisfies

$$M(\alpha_n) \geq \log \left(\frac{r_n}{s_n} \cdot \text{lcm}(s_n, b_{d-1}, \dots, b_1) \right) \geq \log r_n.$$

For each n , let

$$P_n = \{p \in \{p_1, \dots, p_L\} : p \mid r_n\}.$$

We have assumed that $\alpha_1, \dots, \alpha_N$ attains the infimum in $M_t(D^{1/k})$, so we get that

$$(3.5) \quad M_t(D^{1/k})^t = \sum_{n=1}^N M(\alpha_n)^t \geq \sum_{n=1}^N (\log r_n)^t \geq \sum_{n=1}^N \left(\sum_{p \in P_n} \log p \right)^t.$$

Since $t \geq 1$, we always have that

$$(3.6) \quad \left(\sum_{p \in P_n} \log p \right)^t \geq \sum_{p \in P_n} (\log p)^t,$$

which implies that

$$M_t(D^{1/k})^t \geq \sum_{n=1}^N \sum_{p \in P_n} (\log p)^t.$$

However, applying (3.4), we know that for each $\ell \in \{1, \dots, L\}$, there exists $n \in \{1, \dots, N\}$ such that $p_\ell \in P_n$, establishing (3.2) and the first statement of the lemma.

Now assume that $t > 1$. If $|P_n| \geq 2$, then we must have strict inequality in (3.6). Therefore, if $|P_n| \geq 2$ for some n , then (3.5) implies that

$$M_t(D^{1/k})^t > \sum_{n=1}^N \sum_{p \in P_n} (\log p)^t \geq \sum_{\ell=1}^L (\log p_\ell)^t$$

contradicting (3.1). Therefore, $|P_n| \leq 1$ for every n and we have established that

- (a) For every ℓ , there exists n such that $p_\ell \mid r_n$, and
- (b) If $\ell_1 \neq \ell_2$ then we can never have that $p_{\ell_1} \mid r_n$ and $p_{\ell_2} \mid r_n$.

It follows from the box principle that $N \geq L$. Moreover, we may reorder $\alpha_1, \dots, \alpha_N$ such that $p_n \mid r_n$ for all $1 \leq n \leq L$, which shows that

$$(3.7) \quad M(\alpha_n) \geq \log r_n \geq \log p_n \quad \text{for } 1 \leq n \leq L.$$

If we have strict inequality in (3.7) for some n , then

$$(3.8) \quad M_t(D^{1/k})^t = \sum_{n=1}^N M(\alpha_n)^t > \sum_{\ell=1}^L (\log p_\ell)^t$$

contradicting (3.1) and establishing (i). Similarly, if $M(\alpha_n) > 0$ for some $n > L$, then (3.8) holds as well verifying (ii). □

Now that we have proven Lemma 3.1, the proof of Theorem 1.4 is essentially complete. Indeed, when $t \in [1, \infty)$ Theorem 1.4 is simply the first statement of Lemma 3.1, and the case $t = \infty$ was given already in [4]. The only task remaining is to prove Theorem 1.3, in which the second statement of Lemma 3.1 plays a key role.

Before proceeding, we establish some conventions that will be used for the remainder of this article. For $d \in \mathbb{Z}$ and $r \in \mathbb{Q}$, we say that d *divides* r if when r is written $r = m/n$ with $m \in \mathbb{N}$, $n \in \mathbb{Z} \setminus \{0\}$ and $(m, n) = 1$, then either $d \mid m$ or $d \mid n$. We say that d *divides the numerator or denominator of* r if d divides m or n , respectively.

We say that an algebraic number α is *stable* if all of its conjugates lie either inside the open unit disk, on the unit circle, or outside the closed unit disk. Otherwise, we say that α is *unstable*. It is clear that all rational numbers and all imaginary quadratic numbers are stable, while real quadratic numbers can be either stable or unstable. If α is any algebraic number having minimal polynomial

$$f(x) = a_N x^N + \dots + a_1 x + a_0,$$

then it is simple to verify that

$$M(\alpha) \geq \log \max\{|a_N|, |a_0|\}$$

with equality if and only if α is stable. We now state a simple criterion which allows us to determine if a quadratic algebraic number is stable by considering the coefficients of the minimal polynomial.

Lemma 3.2. *Suppose that α is a quadratic algebraic number having minimal polynomial $f(x) = ax^2 + bx + c$ over \mathbb{Z} . We have that α is stable if and only if $|a+c| > |b|$. In this situation, the following hold.*

- (i) *If $|a| < |c|$ then both conjugates of α have modulus greater than one.*
- (ii) *If $|a| = |c|$ then both conjugates of α have modulus one.*
- (iii) *If $|a| > |c|$ then both conjugates of α have modulus less than one.*

Proof. Suppose that $f(x) = a(x - \alpha)(x - \beta)$. If $f(1)$ and $f(-1)$ have opposite signs, then f has precisely one root in the interval $(-1, 1)$. The other root must also be real and lie outside of $(-1, 1)$, so α is unstable. If $f(1)$ and $f(-1)$ have the same sign, then f has either zero or two roots in $(-1, 1)$. In the case of two roots in $(-1, 1)$, α is clearly stable. If f has zero roots in $(-1, 1)$, then it either has two complex roots, in which case α is certainly stable, or two real roots both lying outside of $[-1, 1]$, also implying that α is stable.

We have now shown that α is stable if and only if $f(1) = a + b + c$ and $f(-1) = a - b + c$ have the same sign. Clearly, $f(1)$ and $f(-1)$ are both positive if and only if $a + c > |b|$ and both negative if and only if $-a - c > |b|$. Thus, α is stable if and only if $|a + c| > |b|$.

If, in addition, $|a| < |c|$, then $|\alpha\beta| = |c|/|a| > 1$, so both α and β have modulus greater than 1. Similarly, if $|a| > |c|$, then $|\alpha\beta| = |c|/|a| < 1$ implying that both α and β have modulus less than 1. Finally, if $|a| = |c|$ then $|\alpha\beta| = 1$. Since α is stable, α and β must be complex conjugate numbers both of modulus 1. \square

The following lemma shows us that certain quadratic algebraic numbers, which we will encounter in the proof of Theorem 1.3, have relatively simple minimal polynomials.

Lemma 3.3. *Let D be a square-free integer, p be a prime divisor of D , and α a quadratic algebraic number in $\mathbb{Q}(\sqrt{D})$. If $M(\alpha) \leq \log p$ and p divides the numerator of $\text{Norm}_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\alpha)$ then α is stable. Moreover, the minimal polynomial of α satisfies*

$$f(x) = ax^2 \pm p \quad \text{or} \quad f(x) = ax^2 \pm px + p$$

where a is a positive integer with $a < p$.

Proof. Suppose that $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ is the minimal polynomial of α over \mathbb{Z} , so we may assume that $a > 0$. Since α has degree 2, we have that

$$\text{Norm}_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\alpha) = \alpha\bar{\alpha} = \frac{c}{a}$$

where $\bar{\alpha}$ is the conjugate of α over \mathbb{Q} . We have assumed that p divides the numerator of $\text{Norm}_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\alpha)$, which itself must divide c , implying that $p \mid c$. Since $M(\alpha) \geq \log \max\{|a|, |c|\}$, we have that

$$\log p \leq \log |c| \leq \log \max\{|a|, |c|\} \leq M(\alpha) \leq \log p,$$

and we conclude that

$$(3.9) \quad M(\alpha) = \log |c| = \log p.$$

It now follows that $|a| \leq |c|$ and, since $M(\alpha)$ is the log of an integer, we further obtain that α is stable. Hence, Lemma 3.2 implies that $|a + c| > |b|$.

We cannot have $|a| = |c|$, since

$$\text{Norm}_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\alpha) = \frac{c}{a} = \pm 1$$

is not divisible by p , so it follows that $|a| < |c|$. In view of Lemma 3.2 (i), we have that $|\alpha|, |\bar{\alpha}| > 1$. Therefore, we find that

$$(3.10) \quad |b| < |a + c| \leq |a| + |c| < 2|c| = 2p.$$

Now let $\Delta = b^2 - 4ac$. Since $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{D})$, and D is square-free, we have $\Delta = Dv^2$ for some $v \in \mathbb{Z}$. The quadratic formula gives

$$\text{Norm}_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\alpha) = \alpha\bar{\alpha} = \frac{b^2 - Dv^2}{4a^2},$$

and since $p \mid D$ and the numerator of $\text{Norm}_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\alpha)$, it follows that p divides b^2 . Of course, this implies that $p \mid b$. Using (3.10), we now see that $b \in \{0, p, -p\}$.

If $b = 0$ then we have by (3.9) that $f(x) = ax^2 \pm p$, establishing the lemma in this case. If $b = \pm p$, then $|a + c| > |b|$ holds if and only if a and c has the same sign. So in this situation, (3.9) yields that $c = p$ which leads to $f(x) = ax^2 \pm px + p$. \square

Proof of Theorem 1.3. By Theorem 1.4, we know that

$$M_t(\sqrt{D}) = \begin{cases} \left(\sum_{\ell=1}^L (\log p_\ell)^t \right)^{1/t} & \text{if } t \in (1, \infty) \\ \log p_1 & \text{if } t = \infty. \end{cases}$$

We also observe that

$$(3.11) \quad \sqrt{D} = \sqrt{\frac{p_1}{p_2 \cdots p_L}} \cdot p_2 \cdots p_L$$

and that each term in the product on the right hand side of (3.11) belongs to $\mathbb{Q}(\sqrt{D})$. We obviously have that $M(p_\ell) = \log p_\ell$ for all ℓ . Furthermore, our assumption that $D < p_1^2$ ensures that $p_2 \cdots p_L < p_1$, so it follows that

$$M\left(\sqrt{\frac{p_1}{p_2 \cdots p_L}}\right) = \log p_1.$$

Combining these observations, we see that

$$M\left(\sqrt{\frac{p_1}{p_2 \cdots p_L}}\right)^t + \sum_{\ell=2}^L M(p_\ell)^t = \sum_{\ell=1}^L (\log p_\ell)^t = M_t(\sqrt{D})^t$$

when $1 < t < \infty$ and

$$\max \left\{ M\left(\sqrt{\frac{p_1}{p_2 \cdots p_L}}\right), M(p_2), \dots, M(p_L) \right\} = \log p_1 = M_\infty(\sqrt{D}).$$

establishing one direction of the theorem as well as the second statement.

To prove the other direction, we assume that there exist points $\alpha_1, \dots, \alpha_N \in \mathbb{Q}(\sqrt{D})$ that attain the infimum in $M_t(\sqrt{D})$, and for simplicity, we set $p = p_1$. When $t \in (1, \infty)$, Lemma 3.1 establishes that $M(\alpha_n) \leq \log p$ for all n . In the

case $t = \infty$, we also have $M(\alpha_n) \leq \log p$ for all n as a consequence of Theorem 1.4. Since $\sqrt{D} = \alpha_1 \cdots \alpha_N$, we have that

$$(3.12) \quad -D = \text{Norm}_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\sqrt{D}) = \prod_{n=1}^N \text{Norm}_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\alpha_n).$$

Defining the set

$$\Lambda = \left\{ 1 \leq n \leq N : p \mid \text{Norm}_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\alpha_n) \right\}$$

we apply (3.12) to see that

$$(3.13) \quad \sum_{n \in \Lambda} \nu_p \left(\text{Norm}_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\alpha_n) \right) = \nu_p(D) = 1,$$

where the last equality follows since D is square-free. If Λ contains no irrational points, then we have that

$$p \mid \text{Norm}_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\alpha_n) = \alpha_n^2$$

for all $n \in \Lambda$. However, this implies that $\nu_p(\text{Norm}_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\alpha_n))$ is even for all $n \in \Lambda$. It follows that the left hand side of (3.13) is also even, a contradiction.

We have shown that there must exist n such that α_n is quadratic, $M(\alpha_n) \leq \log p$, and p divides $\text{Norm}_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\alpha_n)$. If p divides the numerator of $\text{Norm}_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\alpha_n)$, then we may apply Lemma 3.3 to see that α_n is stable and is a root of

$$f(x) = ax^2 \pm p \quad \text{or} \quad f(x) = ax^2 \pm px + p$$

for some positive integer $a < p$.

Suppose now that Δ is the discriminant of f . Since α_n is quadratic over \mathbb{Q} , we have $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{D})$. Furthermore, since D is a square-free, we have that $\Delta = Dv^2$ for some $v \in \mathbb{N}$. If $f(x) = ax^2 \pm p$, we see that $\Delta = \pm 4ap$, so that

$$pp_2 \cdots p_L v^2 = Dv^2 = \pm 4ap.$$

Since p_2, \dots, p_L are distinct primes, we obtain that $p_2 \cdots p_L \mid a$, and hence,

$$p_2 \cdots p_L \leq a < p,$$

establishing that $D < p^2$ in this case.

If $f(x) = ax^2 \pm px + p$ then $\Delta = p^2 - 4ap = p(p - 4a)$. We have assume that D is positive so that $p - 4a > 0$, and, trivially, $p - 4a < p$. Hence, $D \leq \Delta = p(p - 4a) < p^2$ completing the proof when p divides the numerator of $\text{Norm}_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\alpha_n)$.

If p divides the denominator of $\text{Norm}_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\alpha_n)$ instead, the p must divide the numerator of $\text{Norm}_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\alpha_n^{-1})$. Of course, we also have that $M(\alpha_n^{-1}) \leq \log p$ and $\alpha_n^{-1} \in \mathbb{Q}(\sqrt{D})$ is quadratic, so we may apply the above argument to α_n^{-1} in place of α_n . \square

REFERENCES

- [1] P. Borwein, E. Dobrowolski and M.J. Mossinghoff, *Lehmer's problem for polynomials with odd coefficients*, Ann. of Math. (2) **166** (2007), no. 2, 347–366.
- [2] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), no. 4, 391–401.
- [3] A. Dubickas and C.J. Smyth, *On the metric Mahler measure*, J. Number Theory **86** (2001), 368–387.
- [4] P. Fili and C.L. Samuels, *On the non-Archimedean metric Mahler measure*, J. Number Theory, **129** (2009), no. 7, 1698–1708.

- [5] D.H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. **34** (1933), 461–479.
- [6] M.J. Mossinghoff, *Algorithms for the determination of polynomials with small Mahler measure*, Ph.D. Thesis, University of Texas at Austin, 1995.
- [7] M.J. Mossinghoff, website, *Lehmer's Problem*, <http://www.cecm.sfu.ca/~mjm/Lehmer>.
- [8] M.J. Mossinghoff, C.G. Pinner and J.D. Vaaler, *Perturbing polynomials with all their roots on the unit circle*, Math. Comp. **67** (1998), 1707–1726.
- [9] M.J. Mossinghoff, G. Rhin and Q. Wu, *Minimal Mahler measures*, Experiment. Math. **17** (2008), no. 4, 451–458.
- [10] D.G. Northcott, *An inequality on the theory of arithmetic on algebraic varieties*, Proc. Cambridge Philos. Soc., **45** (1949), 502–509.
- [11] C.L. Samuels, *The infimum in the metric Mahler measure*, Canad. Math. Bull., to appear.
- [12] C.L. Samuels, *A collection of metric Mahler measures*, J. Ramanujan Math. Soc. **25** (2010), no. 4, 433–456.
- [13] C.L. Samuels, *The parametrized family of metric Mahler measures*, J. Number Theory **131** (2011), no. 6, 1070–1088.
- [14] A. Schinzel, *On the product of the conjugates outside the unit circle of an algebraic number*, Acta Arith. **24** (1973), 385–399. Addendum, ibid. **26** (1975), no. 3, 329–331.
- [15] C.J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. London Math. Soc. **3** (1971), 169–175.

VILNIUS UNIVERSITY, DEPARTMENT OF PROBABILITY THEORY AND NUMBER THEORY, FACULTY OF MATHEMATICS AND INFORMATICS, NAUGARDUKO 24, LT-03225 VILNIUS, LITHUANIA
E-mail address: `jonas.jankauskas@gmail.com`

SIMON FRASER UNIVERSITY, DEPARTMENT OF MATHEMATICS, 8888 UNIVERSITY DRIVE, BURNABY, BC V5A 1S6, CANADA

THE UNIVERSITY OF BRITISH COLUMBIA, DEPARTMENT OF MATHEMATICS, 1984 MATHEMATICS ROAD, VANCOUVER, BC V6T 1Z2, CANADA
E-mail address: `csamuels@math.ubc.ca`